In the Claims:

The claims are as follows:

1-12. (Canceled)

13. (Previously presented) A method for processing a file having an existing filename, said method comprising:

receiving, from a certification authority (CA) who issued a digital certificate, a private key associated with the digital certificate and a certificate address from which the digital certificate may be accessed;

generating a digital signature based on the file and the received private key, said digital certificate comprising a public key associated with the private key such that the generated digital signature can be verified through use of the public key;

signing the file with the generated digital signature;

encoding the received certificate address to generate an encoded address;

merging the existing filename and the encoded address to generate a new filename; and

renaming the file with the new filename.

14. (Previously presented) The method of claim 13, wherein said renaming is performed by a file system, wherein said encoding comprises replacing predetermined characters in the address with associated replacement characters, and wherein the predetermined characters are forbidden by the file system from being used in the new filename.

15. (Previously presented) The method of claim 13, wherein the encoded address is denoted as A, wherein the existing filename is structured as F.E such that F and E respectively represent a first and second sequence of characters, and wherein the new filename is structured as F(A).E.

16. (Previously presented) The method of claim 13, wherein the file comprises a document, wherein said signing the file comprises appending the generated digital signature to the file such that the generated digital signature is disposed between a beginning tag and an ending tag at the beginning of the file before the document.

17. (Previously presented) The method of claim 13, wherein the method further comprises sending the renamed file from an owner of the digital certificate to a user.

18. (Previously presented) The method of claim 13, wherein the encoded address is compressed relative to the certificate address.

19. (Previously presented) The method of claim 13, wherein the certificate address is an address of a server of the certification authority such that the digital certificate is stored in the server.

20. (Previously presented) The method of claim 13, wherein the method further comprises: prior to said receiving, sending a request to the certification authority to issue the digital certificate.

21. (Previously presented) A computer readable medium comprising instructions therein, wherein the instructions are adapted to perform the method of claim 13.

22. (Previously presented) A system comprising:

a computer readable medium comprising instructions therein, wherein the instructions are adapted to perform the method of claim 13; and

means for executing said instructions to perform the method of claim 13.

23. (Previously presented) A method for authenticating a file having a filename that comprises an encoded address, said file comprising a digital signature that was generated based on the file and a private key, said method comprising:

extracting the encoded address from the filename;

decoding the extracted encoded address to generate a certificate address from which a digital certificate may be accessed, said digital certificate comprising a public key associated with the private key, said digital signature being verifiable through use of the public key;

accessing the digital certificate from the generated certificate address;

extracting the public key from the accessed digital certificate; and

verifying the digital signature by executing an authentication algorithm in conjunction with the extracted public key.

24. (Previously presented) The method of claim 23, wherein the digital certificate indicates the owner of the digital certificate, and wherein the method further comprises checking the accessed digital certificate to determine an owner of the digital certificate.

25. (Previously presented) The method of claim 23, wherein the certificate address is an address of a server of certification authority (CA) who issued the digital certificate.

26. (Previously presented) The method of claim 23, wherein the filename is structured as F(A).E, wherein A denotes the encoded address, and wherein F and E respectively represent a first and second sequence of characters.

27. (Previously presented) The method of claim 23, wherein the file comprises a document, and wherein the digital signature is disposed between a beginning tag and an ending tag at the beginning of the file before the document.

28. (Previously presented) The method of claim 23, wherein the method further comprises: prior to said extracting, receiving the file from an owner of the digital certificate.

29. (Previously presented) The method of claim 23, wherein the encoded address is compressed relative to the certificate address.

30. (Previously presented) The method of claim 23, wherein the digital certificate identifies the authentication algorithm.

31. (Previously presented) A computer readable medium comprising instructions therein, wherein the instructions are adapted to perform the method of claim 23.

32. (Previously presented) A system comprising:

a computer readable medium comprising instructions therein, wherein the instructions are adapted to perform the method of claim 23; and

means for executing said instructions to perform the method of claim 23.